GLOBALIZATION AND WMD PROLIFERATION NETWORKS: CHALLENGES TO U.S. SECURITY

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA
JUNE 29 – JULY 1, 2005

CONFERENCE SPONSORED BY
THE ADVANCED SYSTEMS AND CONCEPTS OFFICE OF THE DEFENSE THREAT REDUCTION AGENCY

CONFERENCE REPORT
PREPARED BY
JAMES A. RUSSELL AND CHRISTOPHER CLARY

Amb. Ronald Lehman of Lawrence Livermore National Laboratories addresses the audience.

Introduction

From June 29 to July 1, the Center for Contemporary Conflict convened over sixty-five government officials, military officers, civilian analysts, and non-governmental experts to conduct an in-depth examination of the challenges that proliferation networks pose for U.S. security. This project grew out of research conducted last year by James Russell, a senior

lecturer in the Department of National Security Affairs. Mr. Russell led a project sponsored by the Defense Threat Reduction Agency to assess the causes and consequences of the proliferation of weapons of mass destruction (WMD) in the Middle East. Repeatedly during the course of that research, more and more questions arose about how nations organized their procurement efforts and into how third-state and non-state entities assisted in proliferation activities.

The conference identified significant policy and intellectual challenges posed by this phenomenon. How do analysts grapple with emergent, dynamic, and opaque networks? How and when do policymakers intervene? Eight different themes emerged from the three days of deliberation:

(1) How do policymakers develop and implement the tools necessary to combat proliferation networks?

(2) How do analysts understand complex, non-linear, non-hierarchical phenomenon?

(3) What are the trends in the global technology landscape and what do they portend for this problem?

(4) What relationship, if any, does globalization have to the emergence of proliferation networks?

(5) What is the present capacity of non-state actors to employ weapons of mass destruction?

(6) What lessons can be drawn from the Iraqi procurement network?

(7) What lessons can be drawn from the A. Q. Khan proliferation network?

(8) How significant are proliferation networks?

This conference report will examine all eight topics.

The Policy Landscape

The Bush administration has pursued six inter-related strategies in its attempts to combat weapons of mass destruction:

(1) Reinforce the international non-proliferation regime by gaining compliance from key suppliers (notably China and Russia);

(2) Secure existing weapons of mass destruction and skilled personnel through the expansion of bilateral and multilateral cooperative threat reduction programs;

(3) Reform the international non-proliferation regime by preventing the development of nuclear weapons capabilities under the guise of civilian nuclear programs;

(4) Increase the capability and the authority of the United States, along with its friends and allies, to interdict the illegal trade of weapons of mass destruction technology or material (the Proliferation Security Initiative and recent UN Security Council resolutions) and disrupt proliferation networks through increased law enforcement, intelligence, and military cooperation;

(5) Deny, degrade, and, if necessary, destroy WMD technology possessed by states who pose dangers to the United States, its friends, or its allies; and

(6) Dissuade would-be WMD aspirants from initiating acquisition efforts.

The Bush administration has accorded a centrality to combating weapons of mass destruction as an objective of its National Security Strategy, and also a centrality to counterproliferation (rather than nonproliferation) as a tool in that effort.

John Caves, of the National Defense University, was generally favorable in his policy review. He stated, "The Administration's emphasis on action-oriented, multi-disciplined approaches built on expanding coalitions of the willing strikes me as an appropriate response to an urgent and dynamic threat." He credited the administration, in particular, for innovation and flexibility in its work on the Proliferation Security Initiative. His praise, however, was not unequivocal. He noted the difficulties of the Iraq campaign had reduced presently available military options to deal with other proliferation challenges. He argued, "Without a credible threat of force, even if implicit, to back negotiations to rollback WMD programs in North Korea and Iran, it is difficult to imagine those diplomatic efforts succeeding. This puts a premium on what other measures the United States and the international community can employ to stem the further proliferation of WMD capabilities to and from these and other adversaries."

Chaim Braun, of Stanford University's Center for International Security and Cooperation, noted the challenges of bringing different communities from the government in the same room to deal with proliferation challenges. Braun asked, "How do you get intelligence people and export control people to communicate with each other?" As other participants would note, this is not just a challenge of bridging different cultures—which is a non-trivial obstacle—but also requires careful balancing by policymakers. There is a tension between action and observation. In other words, policymakers aware of the transfer of WMD technology, expertise, or material have the choice of watching that transfer to gain a better understanding of both the suppliers and consumers, or they can move to prevent or interdict the transaction. The principle quandary is that premature action is unlikely to have decisive effect on either a proliferation network or a procurement effort. Greater understanding of the structure of a network—achievable only through watching—is often necessary to impair its function. Of course, waiting too long could allow a potential threat to mature, risking the security of the United States and other countries.

This was one of several difficult compromises highlighted in the conference. How do you control dangerous dual-use exports without unnecessarily handicapping U.S. companies? How do you ban dangerous individuals from studying and working in the United States without alienating thousands of legitimate students and workers that have to go through time-consuming and confusing immigration procedures? There is nothing particularly unique about WMD proliferation networks in this regard. Many policy arenas require balance lest the policies quickly turn counterproductive. But the stakes and the tensions appear particularly acute as the U.S. confronts this challenge.

There are further questions about the effectiveness of the policy tools available. As one government analyst noted, "At some point, this becomes a national law enforcement issues, and a lot of these guys have been prosecuted a number of times and they keep doing it." Another government analyst reinforced the point. He noted that many of the key proliferators are either national heroes or successful businessmen in their home country. How do you confront individuals who are given the benefit of the doubt at home? The businessmen may not even be aware they are involved in proscribed activity. In many of the industries related to weapons of mass destruction, there may not be clear dividing lines between licit, grey, and illicit actions. Dr. Santhanam, a former advisor to the Indian nuclear research effort, pointed out that for some nuclear firms, legitimate business opportunities had largely dried up. Firms in these areas represented a particular danger that ought to be watched, he argued.

Thinking about Complexity and Networks

Network phenomena complicate analysts' tasks considerably. As one U.S. government analyst stated, we need to move past viewing "states as ping pong balls" on a Powerpoint slide. Viewing states as unitary actors—billiard balls colliding in the wilderness—hopelessly distorts our view of the reality. Analysts have to be able to deal with varied levels of interactions and relationships. The task is further complicated because these directions are not unidirectional and they are not static. Entity A can transfer technology to Entity B, which can in turn improve that technology in collaboration with Entity C, and transfer it back to Entity A.

Dr. Phil Williams of the University of Pittsburg emphasized the problems common to the study of complex phenomena. The whole can be greater than the sum of the parts and nonlinear dynamics may make it difficult to ascertain a simple cause and effect. Small changes in context can have big effects. Problems can get dramatically better or worse at key "tipping points," referring to work most popularly summarized by Malcolm Gladwell. Network analysis can also offer a way out. There are multiple different reasons to think that key nodes disproportionately affect most networks, an idea captured in Gladwell's concept of connectors, epidemiological studies of "super spreaders," or in Pareto's 80/20 Principle (where 80 percent of the observed

phenomenon is caused by 20 percent of the sample). Removing these key individuals can shatter the network. At the same time, such networks may be quite resistant to random attack. Pareto's Principle works in the inverse, as well: attacks against 80 percent of the nodes will only have marginal impact.

In a separate presentation, Alexander Montgomery of Stanford University, graphically represented different network configurations: a circle (left), star (center), or clique (right).

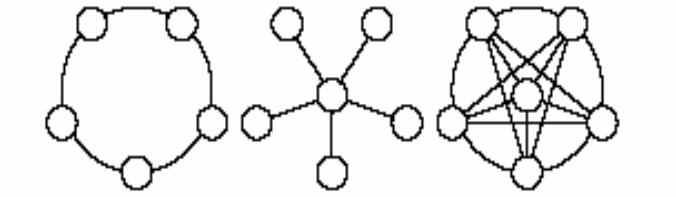

Figure 1: Simple Network Structures

As Montgomery noted, for the star, only the center node must be removed. For a circle or clique, many more nodes must be removed to have total effect. Montgomery continued his analysis, arguing "If the structure is a ring or a clique, then there is no single node (state) that could be shut down to unravel the entire network; consequently, actions against single nodes are likely to be ineffective, while global options—i.e. those that affect all nodes—might seem best. Densely connected, decentralized networks are easier in one sense to shut down: connections to additional nodes in the network are easier to discover. Clique-like networks are highly decentralized—no single state holds a crucial position in the network. But if the structure is a star—i.e. a hub-and-spoke pattern—then the network is highly centralized; efforts are best concentrated on eliminating the central node and preventing other nodes from becoming hubs."

Technological Diffusion

These networks are emerging in a changing technological context. Simply put, deadly technologies are now spreading horizontally and descending vertically. In other words, enabling technologies for WMD are now available in a larger number of states, and they are available to increasingly less capable states and some non-state actors. That statement should not minimize the significant barriers to entry that remain, particularly with regards to nuclear weapons. It does mean that analysts and policymakers must take into account an environment characterized by the seemingly irreversible diffusion of technology.

Dr. Peter R. Lavoy, Director of the Center for Contemporary Conflict, surveyed the present threat environment. He noted that while fissile material production remains challenging and relatively hard to conceal, 14-18 states are researching or are able to enrich uranium; a number that is likely to continue to grow. Similarly, fifteen countries produce ballistic missiles at present, but more are able to and choose not to do so. In addition to a wider threat, newer

missiles are becoming more capable through longer range, better accuracy, and the introduction of solid-fuel propellants. Further, they are become less vulnerable through improved mobility and concealment. The problem is dramatically more widespread in terms of chemical and biological weapons technology. Hundreds of countries have an infrastructure that could be used for chemical weapons production. While only a dozen countries are believed to be pursuing biological weapons, many more could do so.

All of these challenges are exacerbated because of the dual-use nature of many of the underlying technologies. The knowledge and machinery for legitimate enterprise can often be hijacked for dangerous ends. In the chemical and biological world, much of the expertise and equipment is readily available in the private sector. In the nuclear realm, states still retain a heavy degree of control. Even here, however, the network of suppliers that collaborated with A. Q. Khan indicates that significant nuclear-relevant technologies can be acquired from non-state entities. The Khan network provides examples of individuals and firms in South Africa, Malaysia, Dubai, Germany, and the Netherlands. The experience seems to indicate that this is not a geographically bounded problem. This diffusion of science and technology will only continue. Dr. Lavoy noted that 22 out of the 31 most recently constructed nuclear power plants will be built in Asia. Eighteen of the 27 plants now under construction are in Asia.

Corey Hinderstein of the Institute for Science and International Security (left), Zachary Davis of Lawrence Livermore National Laboratories (center), and Scott Sagan (right) of Stanford University enjoy lunch.

Greater numbers of states and non-state entities are developing the indigenous infrastructure and expertise to develop weapons of mass destruction. Ambassador Ronald Lehman of Lawrence Livermore National Laboratories discussed the challenges of such latency, when states have the unexercised potential to develop WMD. He noted that gaining nuclear weapons latency was more difficult than achieving chemical weapons latency, which was in turn more difficult than gaining the latent ability to produce biological weapons. Having such WMD potential

complicates intelligence and policy. Intelligence is forced to gauge intention, which is far more complicated than capability. Simultaneously, the diffusion of technology is likely to lead to significant false positives that tax intelligence assets and may lead to policy mistakes. Policymakers have to work in an environment of greater ambiguity, and may also have to contend with "creeping normalcy," where it is difficult to articulate an actionable threshold to respond to technology acquisition.

This diffusion places export control regime in a bind. As they attempt to gain control over dual-use technologies within the export regime, there are an increasing number of states, firms, and individuals not captured under the old supplier cartel. Export control regimes can expand outwards to secure the cooperation of willing states, but by expanding they are likely to have greater difficulty in gaining consensus and, as a consequence, are likely to be slower in recognizing new threats. This is exacerbated further because export control regimes, by definition, restrict supply, drive up price, and incentivize non-restricted players to enter the marketplace.

Globalization as an Enabler?

Globalization, the process of increasing interconnectedness among worldwide entities, serves as an important backdrop to the emergence of proliferation networks. Dr. Hank Gaffney of the Center for Naval Analyses discounted the relationship between the two phenomena. He argued that globalization was a "very broad, rich, exuberant, sweeping" process, while proliferation has been "small, sneaky, narrow, and happening to countries that are… outcasts in the great world system." For Gaffney, the key analytical question is, "Why so little proliferation despite the huge spread of the global economy?" He contended that the benefits of globalization and the costs of proliferation largely explain these choices. "The question remains: do countries join globalization or not? Do they make those connections or not? Proliferation is a way to opt out, not to join."

Others were less certain. There were three primary impacts attributed to globalization by other participants: obfuscation, avoidance, and enabling. First, increased global trade flows mean a significantly larger number of transactions for intelligence agencies and export controllers to scrutinize. Phil Williams summarized this problem: "[I]n some respects global trade has become more opaque rather than more transparent partly because of its volume, the number of import-export companies, the diversity of freight-forwarders, and the existence of flags of convenience which make the maritime industry itself non-transparent." Williams also pointed to a second problem: jurisdictional arbitrage, where actors "avoid jurisdictions where inspection [is] more stringent and surveillance more intrusive in favor of more permissive countries." Finally, the increasing ease of air travel, financial transactions, and trade may play a

key role in enabling the emergence of complicated, global, proliferation networks. This is complemented by the diffusion of precision manufacturing capabilities to new venues, which themselves are likely to have less experience with export controls. Khan's transactions in Dubai capture many of these phenomena simultaneously. Khan's network ordered parts, through a front company, from a Dubai-based subsidiary of a Malaysian firm. The Malaysian firm, at the direction of Khan's associates, established a factory in Shah Alam, Malaysia in order to fill this order. The factory was provided technical assistance by foreign engineers—old friends of Khan—that would travel to Malaysia periodically to assist with production. The products were then shipped via Dubai to Libya, ultimately being intercepted along the way on the *BBC China*.

James Russell, the principal investigator for this project, discussed the challenge this created for policymakers. Globalization, he argued, had produced ungoverned spaces—holes—in the international system. States were no longer the "major controller or conduit" of global trade, financial, and information flows. This provides space and resources—a metaphorical "dark underbelly"—for non-state actors to exploit. For policymakers, then, the challenges are both spaces that are excluding themselves from the global system—the "gap" identified by Thomas Barnett—and hyperkinetic hubs of the international system, such as the Dubai port, the Hong Kong airport, or banks in the Caymans. As Russell noted, the challenge for states is that they must embrace these flows to remain economically viable. Regulation is like "pushing on a balloon" and only forces these flows back offshore to areas without regulation. This implies global solutions, which often are difficult to negotiate, slow to develop, and sluggish in their response to new threats.

James Russell, principal investigator for the research project, asks a question of the panelists.

The Spoilers: Non-State Threats

A challenge for any analyst of weapons of mass destruction is coming to terms with the non-state actor threat. There is considerable evidence of interest by non-state actors in WMD. There also appears to be good theoretical reasons to suspect that certain WMD capabilities, most notably in the biological and chemical weapons areas, are within the technical and organizational grasp of non-state actors. Nevertheless, there remain few empirical examples of successful attempts by non-state actors to employ these deadly weapons. We asked a series of analysts to discuss some of the unsuccessful efforts about which we know, hopefully to gain insight on future threats.

During the 1990s, there was considerable concern about linkages between organized crime in Russia being able to take advantage of the poorly secured nature of that country's nuclear arsenal. Robert Pajak, formerly of the National Intelligence Council, surveyed these attempts. Pajak noted that so far, these attempts have been rare, relatively amateurish, and of relatively low danger. Pajak argued that criminal organizations, precisely because they are motivated by profit and a desire to persist, are unlikely to undertake actions that might threaten serious reprisals from the state security apparatus. There was debate amongst participants about whether more recent attempts in the former Soviet Union warranted increased concern.

Theft from the former Soviet Union was one of many methods to secure WMD that the Japanese cult Aum Shinrikyo attempted in the early 1990s. Maj. Andrew Groenke, USMC, discussed Aum Shinrikyo's global efforts to acquire and use weapons of mass destruction in attempt to spur Armageddon. From 1991 to 1995, the leadership of Aum made dozens of trips to Russia. As in Japan, they targeted personnel with science and technical backgrounds. They cultivated 35,000 members in Russia, 5,000 of whom lived in Aum facilities. Aum personnel worked in Russian nuclear facilities and Aum paid bribes to high-level Russian executive and legislative officials. Groenke also discussed Aum's efforts in Japan, the United States, and Australia. What is remarkable about the Aum Shinrikyo experience is that their efforts were such a failure. This is despite having enormous assets (perhaps worth over $1 billion) and well-educated members (the professions of the 5 subway attackers were: cardiovascular surgeon, graduate student in particle physics, 2 applied physics graduates, and an electronics engineer). The difficult thing for analysts is whether the Aum experience was unique—a combination of profound luck and organizational dysfunction—or representative of broad challenges that non-state actors face as they attempt to harness destructive technologies.

Dr. Margaret Kosal, a Science Fellow at the Center for International Security and Cooperation of Stanford University, discussed technically less difficult challenges. Her examination of "improvised chemical terrorism" sought to examine near term threats posed non-

state actors. She quoted Milton Leitenberg, of the University of Maryland, who has argued, ""In the real world, there are no known well-trained al-Qaeda scientists." She noted, however, that there are large numbers of well-trained and experienced bomb makers, evident in the fatalities to U.S. forces in Iraq. She also argued that Aum might not be the best example, because there an organization was mimicking a state chemical weapons program. Instead, Kosal argued that chemical terrorism is likely to be a crime of opportunity, from a source familiar with chemicals. Such a conclusion implies a higher likelihood of future chemical terrorist events. Instead of concern about just 50 traditional chemical warfare agents, thousands of known chemicals may present a risk. Further, the number of individuals with the necessary "street chemistry" that could improvise a chemical devise is much larger than those needed to build a sophisticated chemical weapon. Simultaneously, however, such analysis indicates that such a chemical attack is likely to have less serious consequences. Living in this high risk, low consequence environment may still not be particularly satisfying for anyone involved.

Dr. Gerald Epstein, of the Center for Strategic and International Studies, discussed the non-state threat in terms of an expanding challenge from biological weapons. Biotechnology and bioscience, Epstein argued, were expanding in three directions: in the capability and power of the technology, in the depth of market penetration in given economies, and in the breadth of global diffusion. An ever-increasing pool of individuals with biological knowledge is likely to make it progressively easier for terrorist groups to recruit individuals with the information necessary to use a biological agent for malicious ends. Like the latency problem discussed earlier, this complicates the intelligence and policy pictures. For intelligence, it means an increasing number of people, in an increasing number of facilities, with access to the capabilities necessary to make biological weapons. This "background" noise will get louder, making it much more difficult to separate the "signal" from the "static." For policymakers, they are challenged with staying ahead in the offense-defense competition. Epstein offered three reasons defense is difficult: (1) its easier to break things than to fix them; (2) defense has to consider endless vulnerabilities while offense only has to exploit one of them; and (3) defenses operate in a regulatory framework to ensure safety, efficacy, and efficiency. But, as Dr. Epstein noted, "You have to try anyway." He argued for an effort that would leverage the greater transparency and larger numbers and resources of an open and legitimate defense activity.

Iraq: A Case Study

The above discussion has focused on the many ways the threat is growing more complicated. Increasing numbers of states have latent WMD capabilities, non-state actors may have greater success in recruiting the individuals and resources necessary for WMD efforts, and networks of bad actors may lower barriers to entry through the sale of dual-use and proscribed

technologies. Complicating this picture further is the Iraq case, where "we were almost all wrong" about estimates of Iraqi WMD programs. In other words, in the midst of all of these indicators warning analysts and policymakers to be wary of the threat, there is a huge example of the potential of a threat to be exaggerated. Nevertheless, the Iraq case provides perhaps the most data for an exploration of a past procurement network.

Timothy V. McCarthy, who worked on Iraq as a member of the UN Special Commission (UNSCOM) and the Iraq Survey Group, presented on how Iraq structured its procurement effort from the Gulf War in 1991 until the fall of the regime in 2003. He described a system that was adapting to Western efforts to stymie it. From 1991 to 1998, McCarthy described the effort as largely ad hoc—"catch as catch can." In 1999, however, the program experienced a sort of "annus mirabilis." The Saddam Hussein regime was able to capitalize off of larger revenues from the Oil-for-Food program. Combined with this increase in resources, cooperation between the Iraqi Intelligence Service and the Military Industrialization Commission dramatically increased as the result of new leadership. This improvements and others in the procurement network led McCarthy to believe from 2001 onwards, the system was largely up and running in much more sophisticated way than it had been throughout the 1990s. It was redundant, flexible, and adaptive using multiple suppliers, numerous front companies, false end-user certificates, bribery, and other methods to defeat an eroding sanctions regime. McCarthy questioned whether the success of the sanctions regime was sustainable. This evolutionary race between would-be procurers and wannabe deniers is asymmetric. Procuring states are often more determined and seeking to exploit any vulnerability, while denying states have larger resources but often have the ability to defend fewer nodes of potential supply.

For Iraq, the size and the complexity of the effort created a high "noise-to-signal" ratio, where there was a tremendous amount of data for analysts, who had difficulty sorting the useful from the irrelevant. Further, looking at the procurement effort—in many ways the most visible aspect of a WMD program—has its limitations. As Corey Hinderstein of the Institute for Science and International Security pointed out, intercepting a large number of materials does not necessarily indicate a large program, just as intercepting a small number of materials is not necessarily evidence of a small program. Further, procurement activity must still be converted into a technological capability. Even if the Iraqi procurement effort was advancing after 1999, it apparently had not translated into increased capabilities on the ground.

The A. Q. Khan Nuclear Supplier Network

From 1987 to 2003, A. Q. Khan was engaged in a remarkable nuclear enterprise. He provided nuclear technologies to Iran, North Korea, and Libya, and may have offered assistance to Iraq, Syria, and perhaps others. For his "moonlighting," A. Q. Khan earned the distinction of

being “at least as dangerous” as Osama bin Laden, according to former Director of Central Intelligence George Tenet. Grappling with the extent and significance of the Khan network was a recurrent challenge for the participants.

Dr. K. Santhanam, former Chief Advisor (Technology) for the Indian Defense Research and Development Organization. Dr. Santhanam focused his remarks on examining outside assistance previously secured by the Pakistani nuclear program. He continued by detailing outside assistance provided to nearly all nuclear weapons programs. While the scale of the Khan effort is troubling, Dr. Santhanam’s presentation was a reminder that external support is not without precedence. He was dubious that Khan acted as a “rogue element.” He argued, “Scientists and engineers are *on tap, not on top*.”

Dr. Neil Joeck (left) of Lawrence Livermore National Laboratories and Dr. K. Santhanam chat over dinner.

Christopher Clary, research associate at the Center for Contemporary Conflict, presented on Pakistani procurement efforts prior to 1987. He described a multifaceted effort to acquire dual-use components wherever possible. The Pakistani effort was consistently able to stay ahead of the export controls. Pakistan sought uranium enrichment technologies when the nonproliferation regime was focused on the plutonium route. When the supplier cartel grew aware of the purchase of uranium enrichment equipment, the Pakistani effort switched from whole units to sub-systems to major components to sub-components to key precursor materials. As export control lists progressed down on the ladder of components, Pakistan was able to extend its procurement activities for years. He argued that the flexibility and autonomy the Pakistani government provided to Khan in these early years, assisted him as he established his own nuclear enterprise subsequently. Clary also flagged the fact that many of the individuals and firms involved in known proliferation activities in the 1970s and 1980s re-appeared in the most recent incarnation of the Khan proliferation network. He questioned why Western

governments were unable to more effectively track these recidivists and ensure they did not continue to traffic in proscribed technologies.

Corey Hinderstein surveyed Khan's activities from 1987 to 2003. She discussed the evolution from a "highly successful illicit procurement network" to an "organization that could provide 'one-stop shopping' both for the wherewithal to produce weapons-grade uranium and for nuclear weapons designs and instructions." Hinderstein examined efforts to reinforce the global export control regime that have gained momentum after the revelations about the extent of Khan's criminal enterprise. She criticized members of the Nuclear Suppliers Group (NSG) for not controlling proscribed technology emanating from within their borders, and also highlighted the risk posed by states like Malaysia that are outside the NSG, but are still able to produce nuclear-relevant technologies.

Brig. Naeem Salik of Pakistan's Strategic Plans Division (SPD) commented upon the presentations. Salik was able to present unique insights given SPD's role in the command and control of Pakistan's nuclear weapons. He said that Pakistan had learned significantly from the Khan episode: most importantly not to trust any individual as much as they had A. Q. Khan. He examined some of the other mistakes Pakistan had made during these initial phases of its command and control setup, and also detailed changes to Pakistani safety and security arrangements that had been put into place as a result of the investigations into Khan's activities.

Does this Matter? The Significance of Proliferation Networks

The conference recognized that there were limitations to what proliferation networks have done and can do. A. Q. Khan's sales to Libya, for instance, seem to indicate there were still key production bottlenecks that limited the degree of assistance Khan was able to provide. Nevertheless, there was widespread consensus that proliferation networks do represent a significant phenomenon. Specifically, there are at least five related reasons that proliferation networks matter:

1) ***They make WMD acquisition easier:*** Building a WMD program is hard, particularly for nuclear weapons. There has not yet been a high-profile chemical or biological weapons network, akin to the A. Q. Khan affair. But the A. Q. Khan network should be an indicator that there are individuals who are willing to sell dangerous technologies with very few questions asked. Further, as Gerald Epstein, Ronald Lehman, and others pointed out, this technology is becoming more ubiquitous. This increase in technological latency should make it easier for a willing buyer to find a willing seller—or easier for a willing user to recruit personnel willing to supply. As Peter Lavoy noted, even if they do not actually make WMD acquisition easier, they may lead to the perception that WMD

acquisition is feasible. In other words, states that might have forsaken WMD programs as being too costly could now increase their efforts based solely on a (potentially false) perception of greater feasibility. Bringing more players into the game increases the odds that one of them will successfully acquire WMD, while simultaneously diffusing the efforts of a finite pool of policymakers and analysts that seek to manage the problem.

2) ***They make WMD acquisition less detectable:*** As the Iraqi and Libyan efforts demonstrate, attempting to acquire WMD is still a somewhat visible and quite risky affair. With that said, the operation of covert proliferation networks—particularly of difficult to observe technologies like centrifuge enrichment—may give states greater confidence that they can escape or delay detection. Previously, "big ticket items" like reactors provided high-visibility indicators to intelligence communities. By requiring fewer (though by no means insubstantial) indigenous resources, there are fewer indicators for intelligence. Further, as the discussions of latency above indicated, there are increasing levels of "background noise" from legitimate global trade and research. In the proliferation game, only observed programs are costly.

3) ***They may hasten WMD acquisition:*** States often pursue weapons of mass destruction to deal with present threats. Proliferation networks offer a way to leapfrog a generation of research and development, making the prospect of WMD acquisition more immediate and hence more interesting to the contemporary leadership of a country. As Alexander Montgomery has noted elsewhere, it is still unclear the extent to which these proliferation networks have accelerated consumer programs. After all, the Libyan and Iranian examples are still incomplete—without a tested device or even a fully functioning enrichment program. Hinderstein and others argued, however, that it would have taken Iran far more time to develop centrifuge capabilities without Khan's assistance. It is questionable if Libya would have been able to make any significant progress without outside aid. Shorter timelines give intelligence less time to notice the threat, and give policymakers even less time to react.

4) ***They decrease state control over WMD technologies:*** State control of weapons of mass destruction has two principle advantages: (1) it bounds the problem to a relatively small number and (2) it means that WMD have a return address. States still have a presumption of operating in a rational manner. There policies can, presumably, be influenced by outside actors. To the extent that WMD technologies are available to motivated consumers in a private marketplace, the problem set expands dramatically. Further, these buyers and sellers may be more difficult to find and influence. Individuals may be difficult to punish, particularly since law enforcement often requires strict standards of evidence difficult for intelligence agencies to provide—at least without

compromising sources. Non-state actors are likely to be less deterrable than states, though key enablers (accountants, for instance) may still be susceptible to the threat of punishment.

A. Q. Khan would have been unable to set up his procurement network without the assistance of the Pakistani state. Using this state-subsidized infrastructure, Khan was able to develop a technology-exporting network. Khan had a series of middlemen and subcontractors that worked for him, manning key nodes in the operation. There are two critical questions. To what extent do they continue to operate? As Brig. Salik put it, "Let's not miss the forest for a tree. This network of suppliers existed in Europe before Khan. And those people are still there. So Khan has been disposed of, but I don't know what has happened to the others." The second question is to what extent they can provide WMD assistance. One government analyst argued that the technology had been transmitted largely to subcontractors and was outside of state control. There is at least a silver lining to this loss of state control. Ted Warner, former Assistant Secretary of Defense for Strategy and Threat Reduction, commented that at least the "subcontractors aren't national heroes." They may be more vulnerable to action since they are less likely to be (as) protected by their host governments.

5) ***They continue the erosion of the export control regime:*** Like most slippery slopes, the erosion of the export control regime has been long lamented. Technological changes and adversarial innovations continually make and exploit gaps in the nonproliferation regime. Members of the supplier cartel, to varying degrees, attempt to shore up the regime in the face of such erosion. Proliferation networks are simply the most recent innovation in this offense-defense struggle. All of the above seems to indicate that the proliferators currently have the advantage against the controllers. While the export control regime does not appear near collapse, it may be less able to prevent emerging threats. Policymakers will be forced to employ other, more costly tools.

Agenda for Research

The conference helped outline a new agenda for research for the Center for Contemporary Conflict. More work needs to be done on examining the relationships within proliferation networks and between different networks. The availability and significance of dual-use technologies needs to be better studied and understood. Significantly, more lessons need to be drawn from past procurement networks. This event only fleshed out two such networks (the Iraqi procurement network and the Khan proliferation network). There are numerous other examples, however, that carry with them a wealth of data and lessons. The Center for Contemporary Conflict is eager to explore these challenges further in the coming year.